WHAT IS CLAIMED IS:

1.   1. A method of for altering secured data on a storage medium, the method comprising:

2.   establishing a secure session with a host;

3.   receiving, via a communications channel, a command to unlock the secured data

4.   governed by at least one of a plurality of content storage models; and

5.   unlocking the secured data wherein the command responds to an identifier on the

6.   medium, the identifier configured to govern access to the secured data, and at

7.   least one of the plurality of content storage models is a secure content

8.   manager.

1.   2. The method of claim 1 wherein establishing a secure session with a host includes

2.   authenticating the host via a communications channel.

1.   3. The method of claim 1 wherein establishing a secure session with a host includes

2.   transmitting authentication data to the host.

1.   4. The method of claim 1 further comprising receiving from the host an indication of

2.   which data is to be unlocked.

1.   5. The method of claim 1 further comprising determining which data is to be unlocked

2.   by traversing a directory structure and noting secured data.

1.   6. The method of claim 1 wherein the secure content manager is a digital rights

2.   management protocol.

1.   7. The method of claim 1 wherein the plurality of content storage models includes two

2.   or more digital rights management protocols.

1.   8. The method of claim 1 wherein the secure content manager is one of a proprietary and

2.   a third party digital rights management protocol.

1.   9. The method of claim 1 wherein the access to the data is also governed by a file

2.   system.

1   10. A system configured to unlock secured data on a storage medium, the system

2   comprising:

3   a plurality of content storage models for secured data stored on the storage medium;

4   and

5   an engine capable of unlocking secured data wherein the engine modifies attributes of

6   the data on the storage medium to unlock the secured data according to a

7   content storage model in response to a command to unlock the data.

1   11. The system of claim 10 wherein the engine receives the command to unlock the data

2   in a message received via a communications channel.

1   12. The system of claim 11 wherein the communications channel is one of an Internet

2   channel, a satellite communications channel, a wireless channel, and a wired channel..

1   13. The system of claim 11 wherein the message is encrypted.

1   14. The system of claim 10 wherein the plurality of content storage models includes two

2   or more digital rights management protocols.

1   15. The system of claim 10 wherein the content storage model is one of a proprietary and

2   a third party digital rights management protocol.

1   16. The system of claim 10 wherein the access to the data is also governed by a file

2   system.

1   17. A computer program product, comprising:

2   a storage medium;

3   a plurality of content storage models for data stored on the storage medium;

4   a computer program, the computer program comprising:

5   instructions for unlocking secured data according to at least one of the plurality of

6   content storage models by modifying attributes of the data on the storage

7   medium;

8   instructions for communicating with a host via a communications channel; and

9   instructions for receiving from the host a command to unlock the secured data.

1   18. The computer program product of claim 17, wherein the communications channel is

2   one of an Internet channel, a satellite communications channel, a wireless channel, and a

3   wired channel.

1   19. The computer program product of claim 17, wherein the computer program further

2   includes instructions for determining which data is to be unlocked by traversing a

3   directory structure and identifying secured data.

1   20. The computer program product of claim 17, wherein the computer program further

2   includes instructions for establishing a secure session with the host.

1   21. The computer program product of claim 17, wherein the computer program further

2   includes instructions for decrypting the command to unlock the secured data.

1   22. The computer program product of claim 17, wherein the plurality of content storage

2   models includes two or more digital rights management protocols.

1   23. The computer program product of claim 17, wherein at least one of the plurality of

2   content storage models is one of a proprietary and a third party digital rights management

3   protocol.

1   24. An apparatus for unlocking secured data on a storage medium, the apparatus

2   comprising:

3   means for establishing a secure session with a host;

4   means for receiving, via a communications channel, a command to unlock the secured

5   data being governed by a plurality of content storage models; and

6   means for unlocking the secured data on the storage medium wherein the command

7   responds to an identifier on the medium, the identifier configured to govern

8   access to the secured data, and at least one of the plurality of content storage

9   models is a secure content manager.